



**5 February 2020**

**Senior Lieutenant General To Lam**

Minister of Public and Security  
44 Yet Kieu Str., Hoan Kiem Dist., Hanoi, Vietnam

**Cc: Mr. Nguyen Minh Chinh**

Director General of the Cyber Security and High-tech Crime Prevention Department (A05)  
Ministry of Public Security  
45 Hang Bai Str., Hoan Kiem Dist., Hanoi

**Subject: Comments on Outline of Draft Decree on Personal Data Protection**

Dear Minister To Lam,

The Asia Internet Coalition (AIC) and its members express our sincere gratitude to the Ministry of Public Security (“MOPS”) and the Government of Vietnam for the opportunity to submit comments on **Outline of Draft Decree on Personal Data Protection (“Draft Outline”)**.

The AIC is an industry association comprised of leading Internet and technology companies. AIC seeks to promote the understanding and resolution of Internet and ICT policy issues in the Asia Pacific region. Our member companies would like to assure MOPS that they will continue to actively contribute to the security of digital platforms, products and services in support of the digital economy goals of Vietnam. Our members are Airbnb, Amazon, Apple, Expedia Group, Facebook, Google, Grab, LinkedIn, LINE, Rakuten, Twitter and Yahoo (Verizon Media), and Booking.com.

We commend MOPS and the Government of Vietnam for their efforts on data protection measures. While we support these efforts to develop a legal framework for cyber and information security, we express our concerns on the requirements imposed under the Draft Outline and suggest that they be aligned with the provisions in leading global frameworks such as the EU GDPR. In particular, we recommend that the definition of “personal data” in the Draft Outline be narrowed further and the blanket prohibition on the disclosure of sensitive personal data be lifted. Additionally, the provision for registration of transfer of personal data overseas is concerning as it would disincentivize the free flow of data. We also seek clarity on the roles and responsibilities of data processors, as well as the enforcement strategy for the law.

We urge MOPS and the Government of Vietnam to consider the potential consequences of the Draft Outline in order to prevent any unintended consequences in the longer run. As such, please find appended to this letter detailed comments and recommendations, which we would like MOPS and other relevant agencies to consider when drafting **Decree on Personal Data Protection**. We are grateful to MOPS and the Government of Vietnam for upholding a transparent, multi-stakeholder approach in developing this implementation decree. We further welcome the opportunity to offer our inputs and insights, directly through meetings and participating in the official consultations.

In May 2019, we had also submitted a letter recommending best practices to support the development of the Data Privacy Law in Vietnam. The letter has been added below (in appendix 1) for your reference.

Should you have any questions or need clarification on any of the recommendations, please do not hesitate to contact me directly at [Secretariat@aicasia.org](mailto:Secretariat@aicasia.org) or +65 8739 1490 or +84 165 839 0988. Thank you for your time and consideration.

Sincerely,



**Jeff Paine**  
**Managing Director**  
**Asia Internet Coalition (AIC)**

## **Detailed Comments on Outline of Vietnam Draft Decree on Personal Data Protection**

We commend MOPS and the Government of Vietnam for their efforts on data protection measures. However, the language applied in the draft outline appears to be generally vague and unclear, making it more difficult to interpret some provisions and understand their practical implications. Below are the comments and recommendations we would like to propose so that the legal implications of the decree can be properly understood and assessed.

### **A. Definition of “personal data”**

*The definition of “personal data”* includes information in the form of symbols, numbers, sounds, etc. that belong to individuals.

**Comment:** This is a very broad definition compared to the definition in other privacy laws, which typically only cover information relating to the identification of a person. Under this broader definition, any information generated by a person could be considered personal data protected under the decree, which is over-encompassing and impractical. As a practice, we recommend that parity with EU GDPR on issues like the definition of personal data should be strongly considered by the MOPS.

### **B. Meaning of “registration”**

- *Article 3.2* stipulates that “personal data is collected only to achieve the goal for the main purposes, which are *registered*.”
- *Chapter IV, titled “Measures for Protecting Personal Data Processing,”* contains an article on “Registration of sensitive personal data processing” (Article 26) and “Registration of transfer of personal data [of Vietnamese citizens] overseas” (Article 27).

**Comment:** A requirement to register processing activities with a third party would be extremely burdensome and difficult to comply with in practice (especially for organizations that process a high volume of data). This would have a detrimental effect on operations, a chilling effect on innovation, and would make it more challenging for organizations to access state-of-the-art security services. It would also be out of line with leading privacy frameworks, such as the GDPR. We recommend that parameters of such “registration” should be clarified and should not be overly restrictive or impractical.

Moreover, it is unclear what “registration” means in this context. For example, does registration involve an official process that requires approval by a government entity? Or does it simply require companies to notify the public of these issues (e.g. in a privacy policy)? The former is concerning as it would give the government a significant amount of control over companies’ collection and use of data, which could effectively amount to data localisation.

### C. “Registration” of transfer of personal data overseas

*Article 27* seeks to address “Registration of transfer of personal data [of Vietnamese citizens] overseas.”

**Comment:** As mentioned above, if the contemplated “registration” requires government approval for every transfer, such a requirement would be extremely burdensome and impractical both for the regulator and organisations.

This provision is particularly concerning as it suggests a level of restriction on cross-border data transfers by putting artificial restrictions on transferring to secure processors, which in turn may lead to further breaches.

#### *Negative consequences of data localisation requirements*

##### 1. Create harmful impact on cyber-security

In order to effectively defend against cyber threats, companies protect user data and other critical information via a very small network of highly secure regional and global data centers staffed with uniquely skilled experts who are in scarce supply globally. These centers are equipped with advanced IT infrastructure that provides reliable and secure round-the-clock service. The clustering of highly qualified staff and advanced equipment is a critical factor in the ability of institutions to safeguard data from increasingly sophisticated cyberattacks. Mandating data localization can reduce opportunities for Vietnam, lower service levels, create cyber security risks and raise costs. If data is restricted to remain in one country, multiple data centers would be required in the same country and increased costs would likely be passed along to the consumer.

Information technology systems of some agencies and organizations in Vietnam lack the necessary safety and security measures. Some of them only use firewalls or simple access control programs. These organizations and businesses often do not have a team of cyber security experts to advise leaders and managers. Most security products are

delivered from abroad and in many cases, they have not mastered the technology, especially security solutions.<sup>1</sup>

The purchase and sale of personal data is currently very popular in Vietnam. According to the Ministry of Public Security (MOPS), more than 60 organizations and individuals were involved in the illegal trading and use of personal information and data on cyberspace, including: companies providing technology solutions, real estate brokers, bankers, government agencies, who are able to access to electronic governmental systems in education, healthcare, securities, hospitals.<sup>2</sup>

## 2. Stifle investment and growth in Vietnam

Requiring companies to localize data will discourage investment in many of the business sectors that are driving the highest economic growth opportunities, including ICT, payments and financial services, health care and life sciences, and the sharing economy. These are the same digital economy sectors where continued growth and investments are necessary in order for Vietnam to be competitive and for it to continue its rapid upward economic trajectory. Data localization discourages digital economic investment and growth via three central mechanisms – by lowering cyber security protections and standards for businesses and consumers; by impeding the free flow of data across borders, which is a basic requirement for businesses to digitize and stay competitive; and by running counter to international trade trends, therefore sowing uncertainty and doubt within the business community about whether Vietnam's regulatory ecosystem is a safe environment in which to invest.

## 3. Not serve the objectives of greater privacy protection

Many policymakers mistakenly believe that data is more private and secure when it is stored within a country's borders. This misunderstanding lies at the core of many data localization policies. However, in most instances, data localization mandates do not increase commercial privacy nor data security. Therefore, it is important to recognize that the confidentiality of data does not generally depend on which country the information is stored in, only on the measures used to store it securely. Data security depends on the technical, physical, and administrative controls implemented, regardless of where the data is stored.

## 4. Hinder technology adoption

The increased digitalization of organizations, driven by the rapid adoption of cloud computing and data analytics, has increased the importance of data as an input to commerce, impacting not just information industries, but traditional industries as well. Cloud computing uses Internet access and the ability to move data securely across borders to provide cheaper on-demand computing capacity. This includes basic cloud services such as email, software through to giving users direct access to processing, storage, and other computing resources in the cloud. This reduces the need for up-front investment in IT and the associated costs of maintaining often underused computing power. The benefits of cloud are best realized when there are no data

---

<sup>1</sup> [Report on assessment of some contents propose to develop a decree on personal data protection](#) (The document numbered #5)

<sup>2</sup> [Report on current status of personal data protection](#) (The document numbered #6)

localization restrictions placed on data. Such restrictions undermine the economies of scale as well as the security benefits to be gained from shared computing infrastructure.

#### **D. Reliance on consent as a basis of processing**

*Articles 3.4 and 5.1* suggest that personal data may only be used with the consent of the data subject or permission of the competent authorities or as otherwise provided by law. However, *Article 14* suggests that there may be some circumstances in which personal data may be processed without the consent of the data subject.

**Comment:** A privacy regime which relies primarily on consent as a ground for processing is extremely burdensome (for both data processors and data subjects) and does not necessarily lead to favorable privacy outcomes. Ultimately, a consent-based regime transfers accountability from the personal data processor to the data subject. An over-reliance on consent can also lead to consent fatigue and actually cause data subjects to disengage from their privacy decisions. In order to address these issues, there should be other grounds for processing personal data, such as contractual necessity, legal obligation, vital interests, public task and legitimate interests, in line with international standards. The grounds for processing should take into account factors beyond the consent of the data subjects including processing necessary for emerging technologies (which keep evolving), such as Artificial Intelligence and machine learning.

The GDPR has taken a forward-looking view on this and has allowed for the processing without consent in cases such as (i) where it is necessary for the performance of a contract which has been entered into or to take steps at the request of the data subject prior to entering into a contract; (ii) for protecting vital interests of the data subject or another natural person; or (iii) where the processing is necessary for the purposes of the legitimate interests pursued by the data controller or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject.

#### **E. Blanket prohibition on disclosures**

*Article 8.4* contains blanket prohibitions on the disclosure of personal data in certain circumstances.

**Comment:** These blanket prohibitions are atypical, impractical and do not align with international best practices such as the GDPR. They are also very broadly drafted and not subject to any exceptions. For example, there is a prohibition on disclosing personal data “less than thirty days after breach of contract”. The relevance of a breach of contract to a personal data disclosure is not clear (nor is it clear what contract is being referred to or who may have breached it). Furthermore, the meaning of a “disclosure” is not clear. These prohibitions need to be clarified.

Furthermore, there is a blanket prohibition on the disclosure of sensitive personal data. It will be extremely difficult for companies to comply with this, especially as the definition of “sensitive personal data” includes “gender”. This is more expansive

than the definition in other privacy laws, including the GDPR. The inclusion of “gender” as sensitive personal data is onerous as a lot of data processing activities may include the disclosure of gender information and there are no exceptions to this rule (e.g. if the data subject has consented or if it is necessary for employment or medical reasons).

The decree should also acknowledge that the processing of sensitive data can have incredibly beneficial results for the individual and for society. These benefits include the ability to gain insights into disease control and other general health concerns. To ensure that there are opportunities for these beneficial uses of sensitive data to flourish, instead of a blanket prohibition on the disclosure or processing of sensitive data, there should be thoughtful mechanisms or legal bases to process sensitive data (beyond consent, such as legitimate interests) and exceptions such as when the “information has deliberately been made public by the data subject”, such as that contemplated by South African laws.

#### **F. Responsibilities and liabilities of “Data Processors”**

**Article 2, Definitions:** The draft framework contemplates two types of data processors: “main personal data processor,” and “authorised data processor”. However, the generic term “personal data processor” (which includes both main data processors and authorised data processors) is used in most sections of the decree.

**Comment:** It is unclear based on the current definitions what the term “data processor” refers to. We recommend that a clear distinction is made between “data controller” organizations (i.e. those that have control over or authorizes the processing of any personal data) and “data processor” organizations (i.e. those process personal data on behalf of a data controller).

Data processors generally do not have visibility over a data controller's data or content and also do not have direct relationships with data subjects. Hence, obligations and liabilities imposed on data controllers and processors, need to be appropriately allocated, and further clarified. The responsibilities and liabilities of data processors specified in this draft framework are not consistent with international practices.

It also appears that offshore data processors are required to appoint a representative in Vietnam (Article 4.5), which seems to be an additional obligation taken from the Law on Cybersecurity.

#### **G. Requirement that the data subject be informed about “all activities”**

**Article 3.7** sets out a “personal principle that the data subject will be informed about all activities relating to his/her personal data”.

**Comment:** The scope of this obligation needs to be more clearly defined. If interpreted literally, this requirement could be extremely burdensome for data processors and lead to information overload for data subjects. While a data processor should be transparent about the purposes for which it collects and uses personal data,

it should not be required to notify data subjects of every single activity performed in relation to his or her personal data. The scope of this obligation should be more clearly defined and should be consistent with the transparency requirements in leading global frameworks, such as the GDPR.

## H. Sanctions on violations of law

*Chapter VI* deals with sanctions on violations of the law.

**Comment:** There are currently no details under this section and it is difficult to assess its implications. For any proposed sanction to be imposed, there should be an appeal mechanism to allow the impacted personal data processor to lodge an appeal against both the ruling of violation and the sanction. This is to ensure procedural fairness for those who are impacted by a decision of the enforcer of the data protection law to have a chance to have wrongful decision reviewed by a third party.

A regulatory environment whose primary tool for enforcement is the imposition of penalties, fines, and other sanctions is adversarial, lacks transparency, and hinders collaboration between regulators and controllers. Adopting such an approach may lead to organizations seeking to avoid proactive disclosures, and choosing to keep breaches and other incidents secret, for fear of punishment. Such an approach does not benefit consumers.

An ideal regulatory model demonstrates the key principles of fairness, proportionality, accountability, constructive engagement, and mutual trust. Hence, the approach to enforcement must be characterized by a preference to incentivize maximum voluntary compliance, while reserving penalties and other punitive sanctions as the last resort. The ideal enforcement strategy is guided by the objective of maximizing compliance through dialogue, collaboration, and transparency between the regulator and organizations. The focus must be on penalizing only those clear violations which result in tangible, measurable harm due to the misdeeds of malicious actors.

As such, penalties should be levied only in cases of deliberate, repeated, or egregious violations after the regulator has heard and warned the organization in question. The regulator must look to impose proportionate penalties only when necessary and after warnings and other cooperative measures have proved unsuccessful. In addition, any compensation shall be based on specific, quantifiable monetary losses.

Moreover, the law should provide incentives for organizations who develop and implement accountability programs, whether internal or industry-wide (such as self or co-regulation mechanisms, seals, and certifications). These incentives include allowing for a presumption of compliance which result in a statutory reduction of fines and possible exemptions from penalties.



## **Appendix 1**

*29 May 2019*

Senior Lieutenant General To Lam  
Minister of Ministry of Public Security  
44 Yet Kieu Str., Hoan Kiem District,  
Hanoi City, Vietnam

Major General Nguyen Minh Chinh  
Director General of Cyber Security and Counter-High Tech Crime Department  
Ministry of Public Security  
40 Hàng Bai Str., Hoan Kiem District,  
Hanoi City, Vietnam

### **Subject: Submission on best practices and recommendations for the development of Data Privacy Law in Vietnam**

Dear Minister To Lam:

The Asia Internet Coalition (AIC) and its members express our sincere gratitude to the Ministry of Public Security (MOPS) and the Government of Vietnam for this opportunity to submit this letter and share best practices to support the development of Data Privacy Law in Vietnam. AIC is an industry association comprised of leading Internet and technology companies and seeks to promote the understanding and resolution of Internet, ICT, and cybersecurity policy issues in the Asia Pacific region. Our member companies would like to assure MOPS that they will continue to actively contribute to the security of digital platforms, products and services in support of the digital economy goals of Vietnam.

This input is a follow up to the AIC's representation at the data privacy workshop with the Ministry of Public Security, where your delegation graciously agreed to receive inputs from the industry.

We commend the MOPS and the Government of Vietnam for commencing the drafting of the Data Privacy Law and we support these efforts to develop a legal framework that will help boost technology adoption across sectors – payments and financial services, health and life sciences, transportation and logistics, and e-commerce – where continued development and investment are necessary for Vietnam to stay competitive and continue its rapid upward economic trajectory.

With a digital revolution that is profoundly transforming our societies, development of a legal framework favouring such transformation is essential and should take into account the inputs of industry stakeholders. We also urge the ministry to engage with local and recognized international experts to shape the contours of the data privacy law in accordance with





accepted global standards to ensure the safe use of social media, and the protection of data and networks. This should involve experience, knowledge and expertise of the public and private sectors, academia and civil society.

As such, please find attached to this letter detailed set of initial comments on best practices that we urge the MOPS to consider and incorporate while framing rules and regulations on data privacy. Importantly, we will appreciate the opportunity to engage in a dialogue with the ministry and the government in general to serve as a useful collaborative platform in designing the data privacy regulatory framework in Vietnam.

Should you have any questions or need clarification on any of the recommendations, please do not hesitate to contact us directly at [Secretariat@aicasia.org](mailto:Secretariat@aicasia.org) or +65 8739 1490 or +84 165 839 0988. Thank you for your time and consideration.

Sincerely,

A handwritten signature in blue ink that reads "Paine".

**Jeff Paine**  
**Managing Director**  
**Asia Internet Coalition (AIC)**

*(Enclosure)*

## RECOMMENDATIONS ON BEST PRACTICES AND PRINCIPLES

Information technology is in the process of transforming Vietnam's economy. With use of personal data driving many of the innovations being brought to market, issues such as individual consent, cross-border data flows and government access to data, have come to the fore. In framing a Data Privacy Law, the government has the opportunity to provide a clear and consistent regulatory environment for personal data protection and data privacy. Personal data protection, including security, confidentiality, and preserving the integrity of data, is a core data management responsibility. We therefore suggest government to adopt a comprehensive, consistent, principles-based, risk-based framework, underpinned by compliance with global standards and best practices. This approach will enable data-driven innovation and not be overly prescriptive, and enable growth of Vietnam's digital economy, impact of which on jobs (146,000 more by 2020), sales (\$10 billion in B2C sales by 2020) and growth (\$5.1 billion increase in GDP from mobile Internet by 2020) is unprecedented.

### I. Key considerations on the development of legal framework

#### a. Risk based approach

Government should create an environment that encourages participation and self-regulation to minimize risk and provide robust personal data protection. The framework should incentivise development and use of privacy enhancing technologies and methods as a part of the risk-based accountability approach – that is the policy should encourage accountability to address risk of harm to individuals rather than establish a prescriptive set of compliance requirements. An example of a well thought out risk-based approach *for public policy* can be found in the APEC Privacy Framework, which recommends adherence to a set of privacy principles: Preventing Harm, Notice, Collection Limitations, Uses of Personal Information, Choice, Integrity of Personal Information, Security Safeguards, Access and Correction and Accountability. The Preventing Harm Principle recognizes a need to prevent misuse of personal information and consequent harm to individuals. Privacy protections, including self-regulatory efforts and education and awareness campaigns, should be designed to prevent harm to individuals from the wrongful collection and misuse of their personal information. Hence, remedies for privacy infringements should be designed to prevent harms resulting from the wrongful collection or misuse of personal information and should be proportionate to the likelihood and severity of any harm.

#### b. Principles-based Approach

Government must consider the privacy rights of a data subject (users) and abide by a set of principles intended to protect those rights. Listed below are principles, which we urge the government to consider and incorporate:

- **Transparency:** give accurate and full information about the purposes of processing, and any other information necessary to guarantee fair processing.
- **Lawful basis:** provide a lawful basis for data processing, i.e., deciding whether and for what purpose the personal data will be processed.

- **Purpose limitation:** personal data may only be collected for specified, explicit and legitimate purposes, and not further processed in a way incompatible with those purposes.
- **Rights of data subjects:** data subjects must be able to access their personal data, and obtain the rectification, erasure or blocking of personal data, subject to reasonable limitations. A person's rights to access, correction, or deletion/de-identification, may be limited in exceptional circumstances, and only to the extent necessary, if exercising such rights would:
  - Compromise the privacy, security, or other rights of the personal information of another individual (for example, when exercising these rights would give a person access to someone else's information);
  - Interfere with law enforcement, judicial proceedings, investigations, existing legal obligations, or efforts to guard against, detect, or investigate malicious, unlawful, or fraudulent activity or enforce contracts;
  - require disproportionate effort, taking into consideration available technology;
  - Disclose the organization's proprietary technology or business insights; or
  - Violate laws or the rights of other individuals.
- **Integrity:** ensure personal data is accurate and kept up to date to the extent necessary for the purposes of use. This principle recognizes maintaining accuracy and completeness of records and keeping them up to date. Making decisions about individuals based on inaccurate, incomplete or out of date information may not be in the interests of individuals or organizations. This Principle also recognizes that these obligations are only required to the extent necessary for the purposes of use.
- **Data security:** implement appropriate measures to protect personal data from accidental or unlawful destruction, accidental loss, alteration, unauthorised disclosure or access.
- **Data retention:** personal data should not be kept for longer than is necessary for the purposes for which it was collected or processed. A safe deletion process should be considered to prevent accidental loss.
- **Interoperability:** Encourage global interoperability through mechanisms allowing for cross-border data flows, avoiding overlapping or inconsistent rules whenever possible.

### c. Consistency with International Standards and Best Practices

A personal data protection framework should leverage international industry standards and best practices. The framework should be technology-neutral to ensure data protection and privacy rules can be applied regardless of the technologies or the economic sector involved. Data governance is most agile and best conducted when it is technology neutral and structured around self-regulation based on international standards and best practices. There

are many security frameworks, best practices, audit standards, and standardized controls that can be referenced, for example:

- Service Organization Controls (SOC) 1/Statement on Standards for Attestation Engagements (SSAE) International Standard on Assurance Engagements (ISAE) 3402 (formerly Statement on Auditing Standards [SAS] No. 70)
- SOC 2
- SOC 3
- International Organization for Standardization (ISO) 27001
- ISO 9001
- ISO 27017
- ISO 27018
- Federal Information Security Management Act (FISMA)
- Federal Risk and Authorization Management Program (FedRAMP)
- Department of Defense Risk Management Framework (DoD RMF, Cloud Security Model)
- Payment Card Industry Data Security Standard (PCI DSS)
- International Traffic in Arms Regulations (ITAR)
- Federal Information Processing Standard (FIPS) 140-2

## **II. Critical issues to be kept in mind**

### **a. Data residency**

Data residency requirements do not effectively serve the objectives of greater privacy protection and regulatory oversight and are harmful as they inhibit access to services of value to consumers and to industries. Countries that enact barriers to data flows make it harder and more expensive for their businesses to gain exposure and to benefit from the ideas, research, technologies, and best practices that accompany data flows and the innovative goods and services that rely on data. Restrictions on cross-border data flows also create trade barriers and impact business models. Studies show that data localization and other barriers to data flows impose significant costs: reducing U.S. GDP by 0.1-0.36%; causing prices for some cloud services in Brazil and the European Union to increase 10.5 to 54%; and reducing GDP by 0.7 to 1.7% in Brazil, China, the European Union, India, Indonesia, Korea, and Vietnam, which have all either proposed or enacted data localization policies.

In contrary, cross-border data flows can enhance data security in technologies such as cloud computing by allowing greater geographic diversity for data storage. Cross-border data flows are essential to trade and gaining the greatest advantage of global economic opportunity. International flow of data contributed USD2.8 trillion to the global economy in 2014, a figure that could reach USD11 trillion by 2025. Over the past decade, data flows have increased world GDP by 10.1%. Thus, enabling cross-border data flows could result in a positive impact on an Vietnam's GDP. This is supported by the evidence that efforts to reduce barriers to cross- border data traffic have been shown to drive growth.

### **b. Legal Access by Law Enforcement**

Most countries have processes (including Mutual Legal Assistance Treaties or MLATs) to enable the transfer of information to other countries in response to appropriate legal requests for information (e.g. relating to criminal acts). Currently, where data is held in another jurisdiction, officials need to rely on the processes under MLATs to obtain access. A MLAT provides a process whereby one country's law enforcement personnel can request information held by a communication service provider in another country. MLATs were originally designed to facilitate sharing evidence in exceptional circumstances and have proved to be ill-suited when responding to regular requests for access to electronic data. A key limit with MLATs is the time taken to respond to a request for data. For example, to obtain data from a U.S.-based company takes approximately 10 months. This is too long in cases where law enforcement needs to respond to international terrorism or cybercrime.

Data localization is a sub-optimal and inefficient option when responding to the challenges facing local law enforcement and in countering the inadequacies of the MLAT process. As outlined above, data localization creates a range of economic and trade costs and can degrade data security.

Instead, two reforms should be considered. The most immediate is reform of the MLAT process to better accommodate requests for electronic data. The second longer term reform is to consider negotiating data sharing agreements—bilaterally or multilaterally.

### *International Data-Sharing Agreement*

An international agreement is needed that provides mechanisms for governments to gain access to data held in another jurisdiction. Such an agreement would require member countries to have similar standards of privacy and human rights protection, to avoid situations in which fulfilment of these requests by one government would undermine its own domestic privacy and human rights standards. An international approach should ultimately provide an incentive for countries to move toward similarly high standards of privacy and human rights protection, as well as due process norms (i.e., showing probable cause) that would need to be satisfied before the data was provided.

In this regard, the proposed U.S.-UK. data-sharing agreement gives U.S. law enforcement access to data held in the United Kingdom concerning U.S. citizens, and vice versa. The agreement would allow U.K. companies to hand over data on U.S. citizens to U.S. law enforcement officials, upon presentation by the U.S. officials of a domestic (U.S.) warrant.

## **III. Global best practices**

### **a. Data Protection in Japan**

In Japan, the Act on Protection of Personal Information (APPI) 2003 applies to both private and public sectors. In September 2016, Japan passed the “Amended Act on the Protection of Personal Information (APPI)” with implementing regulations released in January 2017. Japan's reformed privacy law came into full force May 30, 2017. Key changes under the new law include:

- Establishment of the Personal Information Protection Commission (PPC) which serves as the central supervisory authority for the APPI.
- The revised APPI provides specific guidance on the use of anonymized data (including approved methods for anonymizing data). This provision aims to enable and encourage use of big data analytics in Japan.
- Under the Amended APPI, exemptions have been modified in how the law addresses the transfer of Personal Data to an offshore entity. Specifically, when the counterparty is an offshore entity, the PI Business Operator will be required to either obtain the prior consent of the Subject, or confirm that such transfer of Personal Data will fall under an enumerated exception (the country in which the recipient is located (a) has a legal system that is deemed equivalent to the Japanese personal data protection system, or (b) is designated by the Japanese data protection authority; or the recipient undertakes adequate precautionary measures for the protection of Personal Data, as specified by the Japanese data protection authority).

Along with a significant number of changes, the new law also introduced a white-list concept, which will add Japan to EU's white list and make the EU, Japan's first "white listed" jurisdiction. The EU Commission has an existing white list of countries it has recognized in the past as having an adequate level of personal data protection to the EU. Importantly, Japan's participation in the APEC Cross-Border Privacy Rules scheme (APEC CBPRs), provides an exemption to cross-border rules in the Japanese legislation, where the receiving company is a certified APEC CBPR participant.

#### **b. APEC Privacy Framework and Cross-Border Privacy Rules**

The APEC Privacy Framework and Cross-Border Privacy Rules (CBPR) are a cross-region, principles-based approach which enables governments to develop national data protection laws that are appropriate for their particular circumstances, while ensuring uniform data protection goals are achieved. The APEC Privacy Framework and the CBPR, taken together are a framework for regional cooperation in enforcement of privacy and data protection laws among the 21 APEC member economies. Accountability is a key principle in the APEC Framework. Under the CBPR, accountability resides primarily with the business collecting the data to ensure that data is protected in compliance with the APEC principles. It provides for use of contracts and Binding Corporate Rules to transfer data to third parties or within conglomerates. Under the Rules, the person who collected the personal data is required to either obtain the consent of the data subject or to "exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles." The CBPR does not prohibit transfers to countries that do not have laws compliant with the CBPR. Rather, the CBPR requires the domestic entity transferring the data to another country, to be accountable to ensure the recipient of data protects the data in a manner consistent with the APEC privacy principles. Participation in CBPR is nascent but growing, with Singapore, South Korea, Japan, Canada, US, and Mexico participating, Australia and the Philippines committed to participate and many other APEC governments considering doing so.

#### **c. Data privacy systems enabling transfers of personal information**

*A number of data privacy systems allow transfers of personal information to countries that have laws that provide similar or “adequate” levels of protection to that of the source country. These countries provide examples:*

- i. **Australia:** Australia requires an Australian entity that intends to disclose personal information to an offshore entity to “take such steps as are reasonable in the circumstances to ensure” that the offshore entity complies with the Australia Privacy Principles. When the offshore entity does not comply with these principles, the Australian entity is *accountable* and liable as if it had not complied itself, regardless of whether it had taken reasonable steps to ensure that the offshore entity complied with Australia’s Privacy Act.
- ii. **Canada:** Canada requires the receiving country to have laws that provide *similar protection* to the domestic law.
- iii. **Japan:** Japan establishes a general rule that the subject of the personal information must specifically consent to the transfer of data to an entity outside of Japan unless
  - the receiving party is in a country that has been recognized by Japan’s regulator to have standards for the protection of personal information that are *equivalent* to those required by Japan’s Personal Information Protection Act;
  - the transferring party and receiving party have ensured that the receiving party will handle the personal information appropriately and reasonably based on the intent of the privacy law (i.e., executing a data transfer agreement similar to the Standard Contractual Clauses approved by the European Commission for transfers of personal data outside the European Union); or
  - the receiving party has a certification recognized by the regulator based on an international framework for handling personal information, such as a certification from the APEC forum’s Cross-Border Privacy Rules system.
- iv. **Philippines:** The Philippines holds the Philippine entity liable for compliance, but provides that data may be transferred to another country if there is a contract between the Philippine entity and the entity receiving the data that the receiving entity is required by law or other reasonable means that ensure that the receiving entity will provide a *comparable level of protection*.
- v. **Singapore:** Singapore provides that the transferring entity is required to take appropriate steps to determine that the entity receiving the data is bound by a legally enforceable obligation to provide the transferred data with a *comparable standard of protection*.